Ph.D Title Proposal

on

An Intelligent Novel Resilient approach for Intrusion Detection System in Software Defined Networks

Submitted in partial fulfillment of the requirement
for the award of the Degree of

Doctor of Philosophy

in

Computer Applications

by

Zahirabbas Jainuddin Mulani

under the guidance of

Dr.Suhasini Vijaykumar

Computer Applications
Bharati Vidyapeeth's
Institute of Management and Information Technology
CBD Belapur, Navi Mumbai -400614
University of Mumbai
November 2022

Faculty: Technology(Computer Applications)

Area: Network Security

Topic of Thesis: An Intelligent Novel Resilient approach for Intrusion Detection System in Software Defined Networks

Date of Admission:27.08.2021

Name of Research Centre: Bharati Vidyapeeth's Institute of Management Information Technology, CBD Belpaur Navi Mumbai 400614

Name of Student: Zahirabbas Jainuddin Mulani

Name of Supervisor: Dr.Suhasini Vijaykumar

Signature of Student

Signature of Supervisor 12/11/2022

Signature of Dean R&D

Signature of Principal 12/11/2022

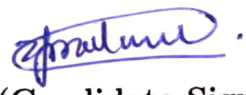
Dr. Suhasini Vijaykumar

PRINCIPAL
Bharati Vidyapeeth's
Institute of Management & Information Technology
Sector-8, C.B.D. Belapur,
Navi Mumbai-400 614

B.V.'s Institute of Management & Information Technology NAVI MUMBAI

Statement by the Candidate

I wish to state that the work embodied in this synopsis titled "An Intelligent Novel Resilient approach for Intrusion Detection System in Software Defined Networks" forms my own contribution to the work carried out under the guidance of Dr. Suhasini Vijaykumar at the Bharti Vidyapeeth's Institute of Management and Information Technology. I declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission.



(Candidate Signature)

Name: Zahirabbas Jainuddin Mulani

Roll Number:

Index

Sr. No	**Contents**
	Abstract
01	Rational and Significance of Study
02	Issues and Challenges
03	A Survey of Work Done in the Research
04	Gap in the Literature Survey
05	Motivation
06	Statement of Aims and Objectives
07	Methodologies and Techniques to be used
08	Plan of Research
09	Outcome Expected
	References

.

Abstract: -

In future very soon, we will be transiting to Software defined networks from the traditional network because software defined networks have numerous application benefits like flexibility, scalability, network-wide visibility and cost-effectiveness. But at the same time, they have massive probabilities of awaiting attacks. Increasing network traffic due to the use of AI, IOT and data science, demands a high instant responsive Intrusion detection system which is the need of the SDN environment, to tackle the most devasting attacks like DOS, eavesdropping, phishing and much more in future. SDN essential components remain the application plane, data plane and control plane out of which control plane is more vulnerable as it's the central part of the networks and the main controller. Due to this, the controller in SDN has gain critical attention of security and also it can be further extended for mitigating the attacks. we will be focusing on few methods from machine learning, deep learning and Swarm Intelligence and the outcome of this systematic literature review-based discussion discloses the dimensions of ongoing challenges in implementing the intrusion detection system for software defined network and help the development of resilient intelligent approach for SDN based security prospective work.

1. Rational and Significance of Study

Due to increase in the applications and data related to AI, Big data, Data science and IOT Traditional network can grow very complex and thus becoming incapable of serving the services. So, there is a birth of new network paradigm called as software defined network which surpasses the other traditional networks. There is a complex dependency among the control plane and the data plane in traditional network operations. This New Software Defined Networking (SDN) separated the planes and provided additional features and tools to solve some of the problems of traditional network like latency, consistency and efficiency [1]. SDN can be stretched to have multiple impressive functionalities like programmability, elasticity, flexibility and adoption capability in network, which are difficult to be realized in traditional network architectures. According to [7] the worldwide market size for SDN is projected to upsurge from USD 13.7 billion in 2020 to USD 32.7 billion by 2025. At present the SDN deployment in incremental and very small [2] but in coming era we will be transiting to Software defined networks from the traditional network because software defined networks because of its such numerous applications. But there are several challenging vulnerabilities which are to be addressed for SDN ascribing to the emergence of virtualization and programmable features. The most destructive kinds of cybercrime are caused by malicious

insiders, denial of service, and web-based attacks. Organizations can lose their intellectual property when malware infiltrates systems can damage a country's critical national infrastructure. Due to increasing global cyber-attacks against government and commercial enterprises Network intrusion detection systems (NIDS) have been developed in academia and industry. The essential purpose of an IDS is to monitor information sources, like computers or networks, for unauthorised access events.

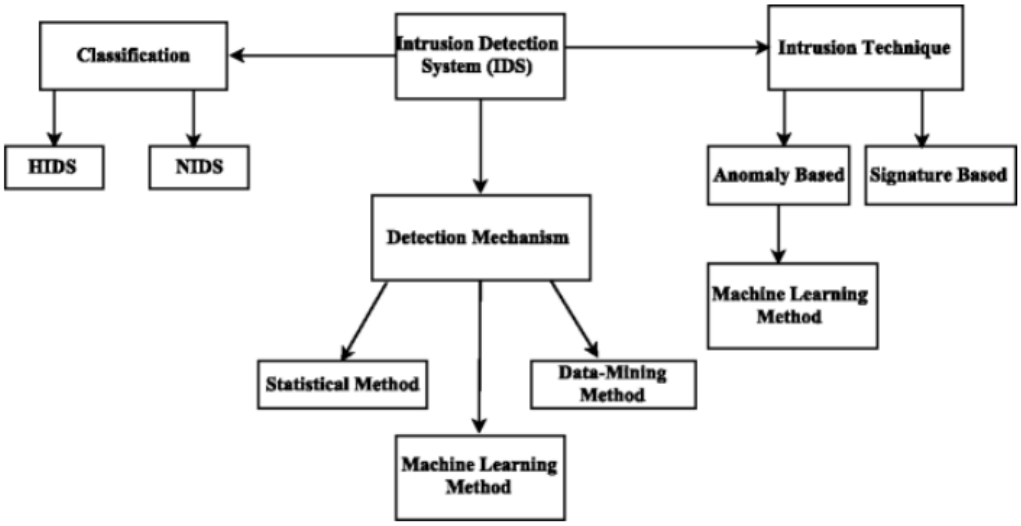


Fig.1 Overview of intrusion detection system

IDS is classified as network-based intrusion detection system and host-based intrusion detection system. Some of the significant Detection mechanisms include statistical, data-mining and machine learning methods. IDS can be implemented using anomaly based, signature based and machine learning based techniques. Anomaly based technique uses baseline compared to normal traffic and activity occurring on the network. we measure the current state of network traffic against this baseline to identify patterns in traffic that are not normally present. Signature based technique detect intruders by observing events and identifying patterns that match known attack signatures. In machine learning, different types of algorithms are used to monitor malicious activities. Various machine learning, deep learning, approaches are implemented for NIDS but little has been done for SDN based NIDS [3]. Also, there is a need of an improvements over these algorithms in many aspects which we will analyse in this study. We also focus on creating an adaptive and rigid approach which will be more intelligent for the intrusion detection system in SDN environment. We will also analyse some of the alternatives for making IDS intelligent enough from swarm intelligence, ensemble learning and fuzzy logic. At the end we focus on application of the Graph neural network for

IDS in SDN for achieving a resilient and agile intelligent approach to detect the malicious activity.

2. **Issues and Challenges**

To provide a context of the contributions of this review, first of all we examined some work related to intrusion detection using various approaches from swarm intelligence to graph neural networks. This was by [4] which proposes an approach to detect and mitigate DDoS attacks using an autonomous multi-agent system with agents using particle swarms. It demonstrates the Optimized performance of the cloud platform and improved security but wasn't for SDN environment and could only detect the DDOS attacks. A feature-pattern graph model [5] substantially outperforms the other methods on precision, recall, and F -score but still there is a scope to improve the method in three ways like automated countermeasure selector to facilitate the selection of countermeasures according to the traffic patterns, to reduce time consumption and computing resources and finally besides flooding-based DDoS attacks, various kinds of DDoS attacks should be considered to make it effective and serviceable in practical use. These DDoS attack patterns are divided into three types on the basis of the protocol type, i.e., ICMP, UDP, and TCP. Unique ensemble framework [11] can effectively detect different attack categories and enhances the detection accuracy of many attack categories in comparison to Deep Learning, Machine Learning, and the Voting ensemble approaches. In [19] authors explored an in-depth overview of the notable published articles from 2015 to 2021 that used Machine Learning (ML) and Deep Learning (DL) techniques to construct an IDS solution in SDN. These studies extended the future research problems such as single controller issue, bottleneck creation due to lack of scalability, evaluation and testing, proper model selection study, lack of SDN specific dataset for model training, additional focus towards detection rather than mitigation and prevention approach, lack of low-rate DDOS attack detection.

3. A Survey of Work Done in the Research

This work not just examines the working and results of existing models for Interruption Location in Programming characterized networks but does a careful basic examination of the equivalent to gain proficiency with their viability and deficiencies in learning and proposing new ways for settling something very similar.

Ref	Type of Intrusion	Techniques	Proposed Solution	Mechanism	Drawback	Future work
Kesavamoorthy et al. [4]	DDOS in cloud	particle swarm optimization	using autonomous multi agent system - particle swarm	can prevent against various kinds of DDoS attacks with the accuracy of the 98%	minimum attack detection and recovery time	optimization using the stochastic based filtering in the attacks detection phase
Xiao et al. [5]	DDOS in SDN	a feature-pattern graph model.	attack behaviour discovery and graph update tasks	malicious attack patterns can be divided as ICMP, UDP, and TCP	Other types of DDoS attack are not considered in this work.	to improve the method and make it effective and serviceable in practical use
Seth et al [11]	Malicious Intrusion	Ensemble machine learning model	effectively detect different attack categories	ability of different base classifiers to identify various types of attacks	ensembles cost more to create, train, and deploy	unsupervised learning to train models on unlabelled datasets in the security
Ahmed et al [19]	Malicious Intrusion in SDN	Machine Learning & Deep Learning	articles from 2015 to 2021 that used Machine Learning (ML) and Deep Learning (DL)	automated IDS utilizing various MLDL algorithms in the SDN paradigm	NA	Single Controller, Lack of Scalability, Lack of SDN Specific Dataset, attack Mitigation, Low-Rate DDoS Attack Detection
Gupta et al [6]	DDoS	Machine Learning	review of various machine learning approaches in SDN	Review	NA	use of Fuzzy logic for DDoS detection in SDN
Thakkar et al [13]	Intrusion Detection	ML, DL techniques, and swarm and evolutionary algorithms (SWEVO).	A survey of feature selection, model, performance measures, application perspective	ML, DL & SWEVO	limitations of each of the dataset	will reinforce the study to explore different capabilities for using and leveraging the information provided in context with attack detection
Banitalebi et al [14]	DDoS	entropy based ML methods	collector, entropy-based and classification	detecting high-volume and low-volume DDoS attacks	attacks detected only by one controller	method can be improved in networks by involving more than one controller
Mahfouz et al [15]	Intrusion Detection	ensemble and adaptive classifier ML model	Intrusion Detection Using a Novel Network Attack Dataset	attacks such as botnet, brute force, DDoS, and infiltration attacks	completely labelled, and about 84 network traffic features have been extracted	improve detection accuracy, improve TPR, and decrease FPR.
Maleh et al [17]	Intrusion Detection	ML	Several vulnerabilities were discovered and exploited	Review	NA	requiring new defence mechanisms
Elsayed et al[18]	Intrusion Detection	ML	to generate an attack-specific SDN dataset	Review	NA	to create a more intrinsic dataset generated from large-scale networks.
Maheshwari et al [20]	DDoS	ML Ensemble	a novel optimized weighted voting ensemble	ensemble framework	NA	explore novel ways of designing dynamic existing metaheuristic optimization algorithms and use them in different domains to create efficient systems

There are a few surveys that have a typical concentration however in [21] creators have proposed a diagram, that licenses catching both the edge elements of a chart as well as the topological data for network interruption location in IoT organizations. It is the first fruitful, functional, and broadly assessed approach to applying GNNs to the issue of organization interruption discovery for IoT utilizing stream-based information.

In [23] a novel GNN architecture is specifically designed to learn and generalize over the previous graph-structured information which shows a comparable result to state-of-the-art ML-based NIDS in the well-known CIC-IDS2017 dataset. These proposed GNN model is completely robust to these attacks, state-of-the-art ML models for NIDS degrade their accuracy up to 50%. The proposed GNN model has the capability to learn the inherent structural flow patterns that compose different attacks. These structural patterns represent a deeper knowledge about attacks, as they typically remain unchanged over time, and across different networks.

According to [24] Experiments on the KDD Cup 1999, NSL-KDD, and UNSW-NB15 datasets achieved accuracies of 99.5%, 97.39%, and 99.9%, respectively.

Proposed RNN-SDR employs a minimum number of features when compared with other models. In addition, the experiments also validated that the RNN-SDR model does not significantly affect network performance in comparison with other options. Based on the analysis of the results, the RNN-SDR model is a promising approach for intrusion detection in SDN environments.

It is observed that there is a need of optimizing the attack detection phase using the stochastic based filtering. The review also claims to improve the method and make it more effective unsupervised learning which will train models on unlabelled datasets in the security. Other issues revealed are like single controller, Lack of Scalability, Lack of SDN Specific Dataset, attack Mitigation, Low-Rate DDoS Attack Detection. There is a great potential to use Fuzzy logic for DDoS detection in SDN, improve accuracy and TPR, and decrease FPR. More intrinsic dataset generated from large-scale networks explore novel ways of designing dynamic existing metaheuristic. Traditional machine learning methods have been replaced by a new approach, called deep learning (DL), RNN and GNN that gives better accuracy when compared with traditional machine learning.

4.Gap in the Literature Survey

From the review of various research articles, it is observed that apart from the performance parameters there are serious security issues related to SDN.

- Existing ML-based NIDS are barely robust to common adversarial attacks, which limits their applicability to real networks. A fundamental problem of these solutions is that

they treat and classify flows independently. There is a requirement of improving the intrusion system particularly in SDN with respect to developing a novel intelligent algorithm.

- There is no focus on attack mitigation, instead only detection is covered.
- Datasets include the old legacy ones like KDD99, CAIDA (2007), etc and there is an unavailability of high-quality datasets.
- DDoS is given more attention than any other aspect of intrusions and also there is a lack of low-rate DDOS attack detection.

5.Motivation

According to an estimation the global IP traffic would increase threefold by the year 2022.It has 26 percent of increase in the annual growth. The network traffic collected 16 GB for the year 2017 and 50 GB by the year 2022. Presently numerous attacks of various kinds, place the network objectives at risk. Late years have seen an extraordinary flood of vindictive exercises on the Web, prompting significant help disturbances and extreme monetary and protection suggestions. For instance, as per [22] the typical expense of an information break in 2020 was $3.86 million, while digital assaults had an expected expense for the U.S. economy between $57 billion and $109 billion just during 2016.Intrusion Detection System (IDS) was developed to recognize the outbreak of a stream of attacks and notify the network system administrator providing network security. IDS is a predictive model used to identify network traffic as routine or attack. An intruder can take over unauthorized access, masquerading, eavesdropping, or injecting malicious code. A system can be harmed by the people who are inside the network by exploiting the vulnerabilities of software application and/or the server that might compromise the system. Software-Defined Networks (SDN) is a revolutionary paradigm that isolates the control plane from the data plane, transforming the concept of a software-driven network which is based on OpenFlow (OF) protocol. Worldwide market size for SDN is estimated to rise up to USD 32.7 billion by 2025.SDN adds efficient and cost-effective functionalities to traditional network as programmability, elasticity, flexibility & adoption capability. But the other side also have a wide range of vulnerability for SDN. Even though machine learning and deep learning gives a better solution for the intrusion detection but still there is a requirement for improvisation. Software Defined Networking (SDN) is a promising architype that permits the programming of the logic behind the network's operation with some abstraction level from the fundamental networking devices. Huge companies, such as Google, already deploy SDN with great success.

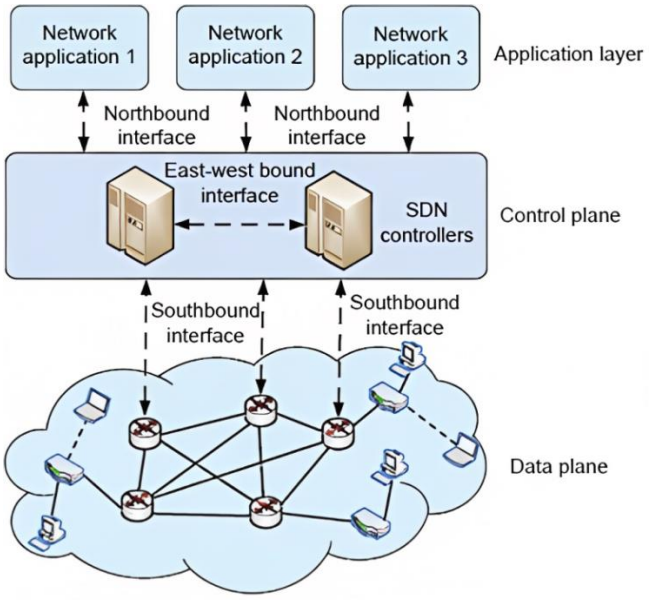


Fig.2 Software Defined Networks Architecture

An SDN architecture delivers a centralized, programmable network and consists of the following:

A controller, the core element of an SDN architecture, that enables centralized management and control, automation, and policy enforcement across physical and virtual network environments.

Southbound APIs that relay information between the controller and the individual network devices (such as switches, access points, routers, and firewalls).

Northbound APIs that relay information between the controller and the applications and policy engines, to which an SDN looks like a single logical network device

SDN architecture and Network Function Virtualization (NFV) architecture depicts network abstraction, nevertheless both the architectures accomplish the network abstraction inversely, which includes virtualization of many networking functions like MME, firewall, IDS, DNS while, SDN forwards the data packet from one network to another network [9].

It also provides a function for routing. Below snap is from the Mininet environment which shows the network automation in terms of a python code which creates the network devices.

```
from mininet.topo import Topo

class MyFirstTopo( Topo ):
    "Simple topology example."
    def __init__( self ):
        "Create custom topo."
        # Initialize topology
        Topo.__init__( self )
        # Add hosts and switches
        h1 = self.addHost( 'h1' )
        h2 = self.addHost( 'h2' )
        h3 = self.addHost( 'h3' )
        h4 = self.addHost( 'h4' )
        leftSwitch = self.addSwitch( 's1' )
        rightSwitch = self.addSwitch( 's2' )
        # Add links
        self.addLink( h1, leftSwitch )
        self.addLink( h2, leftSwitch )
        self.addLink( leftSwitch, rightSwitch )
        self.addLink( rightSwitch, h3 )
        self.addLink( rightSwitch, h4 )

topos = { 'myfirsttopo': ( lambda: MyFirstTopo() ) }
```

Fig.3 Python Code to implement 2 switches and 4 hosts

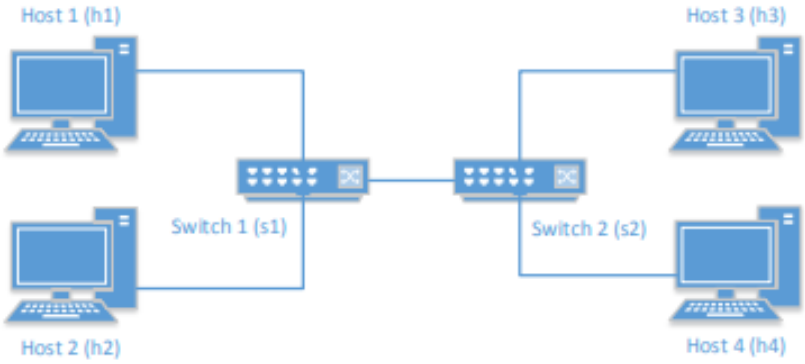


Fig.4 Topology output with 2 switches and 4 hosts

6. Statement of Aims and Objectives

In this proposed research, efforts have been made to explore the various Machine Learning algorithms in SDN and to analyse the design the most productive system. The research plan objectively would generate an improvisation over the present intrusion system in SDN using machine learning and summarily proposed research has the following objectives.

- To recognise and improve an efficient Intrusion detection in Software defined network environment using various advanced Machine Learning algorithms and to propose an intelligent algorithm for enhancing the output.
- To identify a generic independent model towards identifying the abnormal traffic flow from the normal traffic using an improved method of machine learning in Software defined network environment.

- To implement the Intrusion detection approach in SDN on real time traffic using an intelligent approach

7. Methodologies and Techniques to be used

A systematic literature survey is carried out on several facets of the proposed research topic, in various peer-reviewed journals, patents, books and other research resources. This would be followed by documentation, publications and thesis writing.

Simulation in Mininet using POX/RYU controller with the potential of hybrid Advanced Machine Learning Algorithm, for instance like Graph neural network approach with either any existing algorithm or swarm intelligence.

8. Plan of Research

Duration / ***Milestones***	First year				Second year				Third year			
	Quarters				Quarters				Quarters			
	1	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
Identify research area	■											
Formulate research questions		■										
Formulate research strategy, research design and select methods			■									
Define research question			■									
Research proposal				■								
Literature review				■								
Monitor literature and add to review					■							
Publication						■	■	■				
Data set Analysis									■			
Design and Implementation										■		
Simulation											■	
Analysis											■	
Publication									■	■		
Dissertation due												■

9. Expected Outcome

- With the research review of a few articles for SDN security using machine learning, deep learning, and swarm intelligence. The outcome of simulation using Mininet test bed would resolve the dimensions of ongoing challenges in implementing the intrusion detection system for software-defined networks.
- Improved and efficient Intrusion detection in Software defined network environment using various advanced Machine Learning algorithms.
- A generic independent model towards identifying the abnormal traffic flow from the normal traffic using an improved method of machine learning in Software defined network environment.
- Intrusion detection approach in SDN on real time traffic using an intelligent approach probably using a network tool which will create a real time traffic.

References:

1. Rashid Amin , Elisa Rojas , Aqsa Aqdus , Sadia Ramzan, David Casillas-Perez , And Jose M. Arco ,""A Survey on Machine Learning Techniques For Routing Optimization in SDN"", IEEE Access (2021)."
2. Hou Leqing, " How to Realize the Smooth Transition From Traditional Network Architecture to SDN",In 2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), pp. 1948-1952. IEEE, 2020.
3. Sultana, Nasrin, Naveen Chilamkurti, Wei Peng, and Rabei Alhadad. "Survey on SDN based network intrusion detection system using machine learning approaches", Peer-to-Peer Networking and Applications 12, no. 2 (2019): 493-501.
4. Kesavamoorthy R, Ruba Soundar K. "Swarm intelligence based autonomous DDoS attack detection and defense using multi agent system". Cluster Computing. 2019 Jul;22(4):9469-76.
5. Xiao Y, Fan ZJ, Nayak A, Tan CX, "Discovery method for distributed denial-of-service attack behavior in SDNs using a feature-pattern graph model. Frontiers of Information Technology & Electronic Engineering.", 2019 Sep;20(9):1195-208.
6. Gupta, Shaveta, and Dinesh Grover. "A comprehensive review on detection of DDoS attacks using ML in SDN environment." In 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), pp. 1158-1163. IEEE, 2021.
7. Software Defined Networking Market Size, Share and Global Market Forecast to 2025 | COVID-19 Impact Analysis," Marketsandmarkets.com, 2020. [Online]. Available: 14 Feb 2021.
8. Manso, Pedro, José Moura, and Carlos Serrão. "SDN-based intrusion detection system for early detection and mitigation of DDoS attacks." Information 10, no. 3 (2019): 106.
9. Deb, Raktim, and Sudipta Roy. "A comprehensive survey of vulnerability and information security in SDN." Computer Networks (2022): 108802.
10. Feng, Mingjie, Shiwen Mao, and Tao Jiang. "Enhancing the performance of futurewireless networks with software-defined networking." Frontiers of Information Technology & Electronic Engineering 17, no. 7 (2016): 606-619.
11. Seth, Sugandh, Kuljit Kaur Chahal, and Gurvinder Singh, "A novel ensemble framework for an intelligent intrusion detection system.", IEEE Access 9 (2021): 138451-138467.
12. Jayasri, P., A. Atchaya, M. Sanfeeya Parveen, and J. Ramprasath. "Intrusion detection system in software defined networks using machine learning approach." International Journal of Advanced Engineering Research and Science 8, no. 4 (2021): 241-247.
13. Thakkar, Ankit, and Ritika Lohiya. "A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions." Artificial Intelligence Review 55, no. 1 (2022): 453-563.

14. Banitalebi Dehkordi, Afsaneh, MohammadReza Soltanaghaei, and Farsad Zamani Boroujeni. "The DDoS attacks detection through machine learning and statistical methods in SDN." The Journal of Supercomputing 77 (2021): 2383-2415.
15. Mahfouz, Ahmed, Abdullah Abuhussein, Deepak Venugopal, and Sajjan Shiva. "Ensemble classifiers for network intrusion detection using a novel network attack dataset." Future Internet 12, no. 11 (2020): 180.
16. Gupta, Shaveta, and Dinesh Grover. "A comprehensive review on detection of DDoS attacks using ML in SDN environment." In 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), pp. 1158-1163. IEEE, 2021.
17. Maleh, Yassine, Youssef Qasmaoui, Khalid El Gholami, Yassine Sadqi, and Soufyane Mounir. "A comprehensive survey on SDN security: threats, mitigations, and future directions." Journal of Reliable Intelligent Environments (2022): 1-39.
18. Elsayed, M.S., Le-Khac, N.A. and Jurcut, A.D., 2020. InSDN: A novel SDN intrusion dataset. IEEE access, 8, pp.165263-165284.
19. Ahmed, Md, Swakkhar Shatabda, A. K. M. Islam, Md Robin, and Towhidul Islam,"Intrusion Detection System in Software-Defined Networks Using Machine Learning and Deep Learning Techniques–A Comprehensive Survey." (2021).
20. Maheshwari, Aastha, Burhan Mehraj, Mohd Shaad Khan, and Mohd Shaheem Idrisi. "An optimized weighted voting based ensemble model for DDoS attack detection and mitigation in SDN environment." Microprocessors and Microsystems 89 (2022): 104412.
21. Lo, W.W., Layeghy, S., Sarhan, M., Gallagher, M. and Portmann, M., 2022, April. E-graphsage: A graph neural network based intrusion detection system for iot. In NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium (pp. 1-9). IEEE.
22. IBM and the Ponemon Institute. Cost of a Data Breach Report 2020. https://www.ibm.com/security/databreach.
23. Pujol-Perich, David, José Suárez-Varela, Albert Cabellos-Aparicio, and Pere Barlet-Ros. "Unveiling the potential of graph neural networks for robust intrusion detection." *arXiv preprint arXiv:2107.14756* (2021).
24. Albahar, Marwan Ali. "Recurrent neural network model based on a new regularization technique for real-time intrusion detection in SDN environments." Security and Communication Networks 2019 (2019): 1-9.